UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 25-cv-20544-MARTINEZ-SANCHEZ

JAY LEWIS FARROW, FARROW LAW, P.A., DR. JANE DOE, and INFANT DOE, Plaintiffs, vs. IOA GROUP, LLC, INSURANCE OFFICE OF AMERICA, INC., HEATH RITENOUR, JOHN RITENOUR, FTI CONSULTING, INC., STEVEN H. GUNBY, TIMOTHY KOLAYA, STUMPHAUZER, KOLAYA, NADLER & SLOMAN, PLLC, BRIAN MORAN, MORAN, KIDD, LYONS, JOHNSON, GARCIA, P.A., GUNSTER LAW, BENJAMIN WIEDER, MCCLATCHY MEDIA COMPANY, DUANE MORRIS, LLP, JOE TAYLOR RESTORATION, INC., JOSEPH CLIFFORD TAYLOR, WIESS, SEROTA, HELFMAN, COLE & BIERMAN, P.L., DUANE MORRIS, LLP, BUCKNERMILES, P.A., ROIG, ROSENBERG, MARTIN & BELLIDO, P.A., TELAN, MELTZ, WALLACE & EIDE, P.A., AMERICAN CASUALTY COMPANY OF READING, PENNSYLVANIA, BERKSHIRE HATHAWAY SPECIALTY INSURANCE COMPANY, CHUBB CUSTOM INSURANCE COMPANY, HARTFORD CASUALTY INSURANCE COMPANY, MARKEL INSURANCE COMPANY, NATIONWIDE INSURANCE COMPANY OF AMERICA, PHILADELPHIA INDEMNITY INSURANCE COMPANY, and SAFEPOINT INSURANCE COMPANY, Defendants._____	

PLAINTIFFS' VERIFIED MOTION FOR STATUTORY EQUITABLE RELIEF PURSUANT TO THE COMPUTER FRAUD AND ABUSE ACT 18 U.S.C. § 1030(g) AND/OR FLORIDA'S CRIMINAL RICO ACT FLA. STAT § 895.05(6)

COME NOW, Plaintiffs, JAY L. FARROW ("Farrow"), FARROW LAW, P.A., ("FLF" or "Farrow Law"), DR. JANE DOE ("Dr. Doe") and INFANT DOE (collectively "Plaintiffs"), by and through undersigned counsel, and file Plaintiffs' Verified Motion for Statutory Equitable Relief Pursuant to the Computer Fraud and Abuse Act **18 U.S.C. § 1030(g) and/or Florida's Criminal RICO Act Fla. Stat. §895.05(6), and in support thereof, state as follows:**

I. INTRODUCTION

The facts of this case and its implications are truly a watershed moment. In the first instance, here, a mother, father and infant child have been the targets of the end stages of an Advanced Persistent Threat ("APT") Cyber Attack for over eight months - an attack so infamous, menacing, highly sophisticated, and in some instances, deadly, that its perpetrator is usually a hostile nation-state against a government agency or national political campaign. In the second instance, what makes this family's suffering more egregious and this case's impact monumental is that this APT Cyber Attack was used by the Threat Defendants Heath Ritenour, John Ritenour, Insurance Office of America, Inc., IOA Group, LLC, FTI Consulting, Inc. and Steven Gunby and other associates ("Threat Defendants" or "Threat Actors") as a malicious tool to: (1) eliminate an opposing lawyer and law firm from prosecuting them in state and federal court; (2) steal the law firm's files related to their cases; (3) and then sabotaging the firm until it effectively closed through seismic interferences, targeting staff and severing communications.

While the results are terrorizing, how they were achieved should shock the consciences of the members of the cyber, legal and medical communities. More specifically, to effectuate and achieve their Ultimate Goals, the Threat Defendants gained unlawful access to computer networks belonging to nearly 40 different other law firms, the Florida Bar, Florida's eFiling Authority/eFiling Portal, Florida Department of Financial Services, Jackson Memorial Hospital and stole confidential information from and even caused the illegal video recording of regular video conference Florida Lawyers Assistance meetings. And to gain either initial, secondary or stronger computer network footholds, the Threat Actors ***used regular service of pdfs and document exchange links to deliver malware payloads and malicious computer code***. Additionally, the Threat Actors used a sprawling array of means and methods to influence judicial

proceedings, used their breaches into the Florida Bar's Network to fabricate and file a Petition in the Florida Supreme Court for Immediate Suspension of Farrow's law license, blocked Plaintiffs' access to state courts and used their powerful media outlets to ensure that nothing ended their unfettered profiteering through deceptive business practices and criminal conduct.

Unless swift, certain and precise measures are taken here and now, not only will the Threat Actors continue, but every law firm and lawyer will have to now think twice before opening an email from opposing counsel, downloading a correspondence, court filing or discovery document link. In this case, in real time, this Honorable Court is presented with the daunting evolution of the exponential technological advancement of cyber-threats to gain unlawful and unjust advantages in litigation proceedings. Indeed, we are not in "Kansas" anymore as what may have been hiding a needle in a haystack within the proverbial warehouse of 'banker's boxes', has been replaced by packaging invisible syringes full of poisonous malware in a hyperlink.

Malware does not just hide inculpatory evidence, it infiltrates every part of the opposing firm's computer network, runs in the background and is hidden through sophisticated defense evasion techniques. Illegal monitoring strategies, and intercepting internal communications is at issue in this case, yet it is unfortunately, fairly insignificant compared to what was perpetrated from June 3 through July 10, 2024 and thereafter, which was using all of the nefariously implanted architecture and "Crisis Scams" to effectively close Farrow Law in just over four weeks and thereafter repeatedly targeting the mom, dad and their infant child to make sure they did not get up and fight back.

What was once only financially available to sovereign nations, has now become affordable to wealthy criminal organizations whom have discovered that using highly advanced cyber-weaponry to commit their illegal conduct both increases their influence, power and bank accounts while substantially reducing the odds of getting caught. However, the Threat Defendants Heath Ritenour and John Ritenour were 'caught' in 2019 for stealing millions of dollars of insurance commissions and using part of the bounty to manipulate the price of Defendant IOA Group, LLC's stock which has and will providing them ill-gotten windfalls. In June 2019, a month after a lawsuit was filed against them, they made another choice to hire FTI Consulting, Inc. to calm what one insider called a "Boiling Ocean" with one of their corporate crisis management strategies fit for their elite clients, with all the trimmings of corporate espionage through unlawful accessing of protected computers, surveilling legal counsel and their signature social engineering theatrics.

However, in March 2024, FTI and its CEO Steven Gunby were caught illegally influencing legal proceedings for and with Heath Ritenour and John Ritenour, as well as, their other elite clients by using fictitious 'experts' who only existed on FTI's website and social media profiles. When confronted with this evidence in April 2024, Threat Defendants, along with the companies they lead and direct, Threat Defendants IOA, Inc, IOA, LLC and FTI decided that the 'tried and true' litigation process created the risk of not just civil exposure but threated the very existence of the well-oiled criminal empires they respectively for themselves.

In summary, by March 2024, the Threat Defendants had already built fortified footholds in Farrow Law's computer network. On May 28, 2024, Farrow and Farrow Law filed on behalf of their client, an Amended Complaint in a pending federal racketeering lawsuit.[1] On June 3, 2024, Farrow received a call and then a text from an FTI associate taken the day he was born some twenty months prior – and that photo was not taken by Farrow's phone. From June 3, and over the next four weeks, the Threat Defendants caused massive interruptions to Farrow Law's computer network and the firm's communications and functionality. On June 21 and 25, 2024, Farrow filed two emergency motions seeking to restrain the Threat Actors. In their Joint Response, the Threat Actors did not deny anything and arguing, legally, nothing could be done stop them even if they did it. On June 1, 2024, the district court denied the emergency motions, not because it could not see the connections, but, at that time, there was only circumstantial temporal proximity between litigation events and the cyber-attacks.

On July 10, 2024, after 16 ½ years in business, Farrow Law was effectively closed, the files related to prosecuting Threat Defendants were stolen, other client files vandalized and Farrow's communications with staff, clients, friends and colleagues severed. In so doing, not only were the Threat Defendants successful in constructively ending the prosecution of the lawsuits against them, but they also deprived Farrow Law's other clients of legal counsel and files, while simultaneously eliminating the dynamics, structure and security of Farrow, his wife, Dr. Doe and their child, Infant Doe.

Plaintiffs have inched their way through these eight months living through constant and debilitating cyber and non-digital attacks which are described as "***Crisis Scams***" that introduce a situation or event which necessitates emergency action and attention. Each *Crisis Scam* is tailored

[1] Spagnuolo v. American Casualty et al., USDC, S.D.Fla: 24-cv-60422-SMITH-HUNT

to deplete substantial resources, cause extreme emotional distress and physically exhaust, at the end of the day, a mom and dad with a young child – all so that the Threat Defendants can ensure that there is no interruption of their illegal profiteering. The Threat Defendants deploy *Crisis Scams* with no warning, and, as allegedly herein, in substantial part, continue to cause irreparable harm, severe trauma, emotional pain and the verge of complete financial devastation – all of which was and is in service to the Threat Defendants' own purposes of illegal unfettered profiteering.

Since the filing of the Verified Complaint on February 5, 2024, the Threat Defendants have again upped the stakes of their "***Crisis Scams***" by: (1) interfering with Dr. Doe's communications with transplant teams during an active multi-organ transplant on February 7 ,2025; (2) hacking two more cell phones belonging to Farrow and Dr. Doe which are now blocking calls between them and others over the last 4 days hours; (3) interfering with Farrow's communications with the Florida Bar relative to his and Dr. Doe's hand-delivered specific evidence of the breaches into the Florida Bar Network; (4) using their unlawful access to Florida's eFiling Authority to block Farrow from filing court documents related to Farrow and Dr. Doe's legal matters; (5) sending one of Farrow and Farrow Law's clients the most highly personalized email threat that particular client received since June 2024; and (6) Farrow has received four highly sophisticated spear phishing emails initiating a brand new "Crisis Scam" involving litigation filings in old cases (up to 10 years old) which Farrow has no secure means to contact the clients to advise or notify them whatsoever.

Plaintiffs herein argue that there are no other less restrictive stopping the Threat Defendants conduct and activities than suspending, conditionally or otherwise, Heath Ritenour, John Ritenour and Insurance Office of America's Insurance Licenses, and placing a conditional revocation upon the corporate charters of IOA, Inc., IOA Group, LLC and FTI's license to conduct business in Miami-Dade County and this Honorable Court has the statutory power to enter equitable orders to effectuate such suspensions and/or conditional corporate charter revocations pursuant to Florida's Criminal Racketeering Act, "Civil Remedies", Section 895.05(1) and (6). Conjunctively, pursuant to 18 U.S.C. § 1030(g), Plaintiffs request that the Threat Defendants be enjoined from further attempting to or accessing Farrow, Farrow Law or Dr. Doe's protected computers, their email and social media accounts, or any others which are currently being used to threaten significant harm.

II. VERIFIED FACTS SUPPORTING EQUITABLE RELIEF

A. Verified Factual Background

In May 2019, Plaintiffs Jay L. Farrow and Farrow Law filed a lawsuit against Defendants Heath Ritenour, John Ritenour, and Insurance Office of America, Inc. for, *inter alia,* stealing a very large insurance account from one of IOA's Agents and using the substantial ill-gotten gains to manipulate the price of IOA's private stock which exponentially increased the bounty of fraudulent conduct.[2] Thereafter, in June 2019, the Ritenours and IOA hired FTI to plan and execute a corporate crisis management strategy which included a long-term sequence framework process to gather information, infiltrate Farrow Law's computer network, advance network permissions and ultimately use administrator status to achieve specific Ultimate Goals.[3] These Ultimate Goals included stealing Farrow Law's case files, sabotaging the firm's infrastructure and causing its effective closure.[4] Thereafter, these Ultimate Goals were to persist in targeting Plaintiffs and causing them extreme pain and suffering which would ensure the end of any civil or criminal consequences which protected otherwise unfettered illegal profiteering.[5]

In the first few months of 2024, Farrow discovered that the Ritenours, IOA and FTI's conduct and activities had included, *inter alia,* unlawful tampering with discovery documents, illegally influenced judicial proceedings, and bid rigged insurance policies associated with the large stolen account.[6] By late March 2024, the Threat Defendants directed and ordered an exponential escalation of the APT's conduct and activities.[7] Ultimately, on May 28, 2024, Farrow and Farrow Law filed, on behalf of their Client, an Amended Complaint in a federal lawsuit which sought damages and injunctive relief against the Insurance Carriers whom appointed Heath Ritenour and John Ritenour as their Agents, and also, named FTI as a Defendant.[8] From the beginning of June 2024, the Threat Defendants used the footholds within Farrow Law's network to implode its functions, sever communications and to attack the firm's staff with harassment and intimidation.[9]

On June 21 and 25, 2024, due to substantial cyber-attacks which commenced following the filing of an Amended Complaint, Farrow, on behalf of his client and family filed two Emergency

---

[2] Verified Complaint [D.E. 1], ¶ 233, 364-365 and 368.
[3] *Id.* at ¶ 207-223, 215, 368, and 385.
[4] *Id.* at ¶ 208.
[5] *Id.* at ¶ 208.
[6] *Id.* at ¶ 536-540, 556-557, 559
[7] *Id.* at ¶ 611-613, 742-743
[8] *Id.* at ¶ 633; *See also generally* May 28, 2024 Amended Complaint, 2024 Federal Case 24-cv-60422 which is **Exhibit 1**, being filed under Notice of Filing Exhibits to this Motion.
[9] Ver. Comp. at ¶ 632-744

Motions requesting a limited restraining order to stop the unlawful interferences.[10] On June 25, 2024, in their Joint Response, nothing was denied, yet legal arguments made.

On Monday July 1, 2024, the Court denied the emergency relief the injunction standards of substantial likelihood could not be met. On July 8, 2024, Plaintiffs Farrow, Farrow Law, again on behalf of their client, but more so now on behalf Farrow's family which included hand-written verified statements that the cyber-attack had included an incident at Farrow and Dr. Doe's residence where the Coral Gables Police were dispatched after 12:00am. In the July 8 Motion, Farrow requested a live court hearing to present evidence. On July 10, 2024, the Court denied the motion and by that time Farrow's communications were severed with staff, clients and opposing counsel, his IT firm disappeared, and Farrow did not have any access to the internet.[11]

B. Verified Facts of APT Cyber-Attack Sequence Framework Structures

1. Target Selection, Defined Ultimate Goals, Research and Testing

In at least 2020, Plaintiffs Farrow and Farrow Law, followed by Dr. Jane Doe and Infant Doe in 2023, were selected as targets of the Threat Actor's APT.[12] The Plaintiffs were selected for purposes of the Threat Defendants achieving defined Ultimate Goals.[13] Beginning in at least early 2000, the Threat Defendants were engaged in the research and information gathering protocols of an APT, and began testing vulnerabilities.[14]

2. Sophisticated Cyber-Techniques, Tactics and Protocols

In order to achieve, pursue and accomplish their Ultimate Goals the Injunction Defendant used the architectural model of an APT, and used a sprawling array of cyber-Techniques, Tactics and Protocols ("TTPs") which were and are sophisticated in that they demonstrate a high level of cyber expertise and training.[15]

3. Accessing of Protected Computers, Malware Deployment and Remote Access

While undiscovered until June 2024, the Threat Defendants used the cloak of legal proceedings to serve Plaintiffs Farrow and Farrow Law with pdfs and links related to litigation

---

[10] *Id.* at ¶ 680-684; *see also* Plaintiff's Notice of Filing of February 10, 2025 [D.E. 4] ("PNOF4"), Comp. Ex. B(1) June 21, 2024 Emergency Motion and B(2) June 25, 2024 Emergency Motion.
[11] Ver. Comp. ¶ 744.
[12] Ver. Comp., ¶ 234
[13] Ver. Comp., ¶208 and 215.
[14] *Id.* at ¶ 235-236.
[15] *Id.* at ¶244-336, *see also* Expert Report Summary Opinion, **Exhibit 2** being filed separately.

which contained malware packets and/or malicious code which allowed them and/or their operators to build fortifications into Farrow Law's Network and the protected computers attached thereto, as well as, the protected computers belonging to Farrow and Farrow Law's attorneys and those related to Jackson Health, UM Health and/or the Miami Transplant Institute.[16] The Threat Defendants caused unauthorized access into protected computers using malware which allowed them to remotely access those computers from at least March 2021 through present.[17]

4. Defense Evasion, Permission Advancement, Exfiltration and Covering Tracks

The Threat Defendants intentionally used Defense Evasion tactics. The Threat Defendants had the unique qualifications to plan, execute, and finance an APT.[18] The Threat Defendants accomplished substantial all of the sequence framework structures of an APT, from target selection to the theft of data and covering tracks in pursuit of their ultimate goals.[19] In March 2024 through July 2024, the Threat Defendants substantially increased conduct and activities, such as their Crisis Scams, and also their unlawful access into protected computers causing substantial damages. [20]

On July 10, 2024, Farrow Law effectively closed and thereafter, the Threat Defendants have used collateral computer networks and the protected computers connected to those networks to: (1) gain unlawful access to replacement protected computers owned by Farrow, Farrow Law and Dr. Doe; (2) cause Crisis Scams; (3) drain financial, emotional and other resources such as the time Farrow spent on responding to conjured and manufactured legal issues related to Farrow Law's office, with the Florida Bar and remediating the interferences with the prosecution of Plaintiffs claims in state courts by and through unlawful access into Florida's eFiling Authority's network.[21]

C. Verified Facts Related to Plaintiffs' Attempts to Obtain Judicial Remedies, and Cooperation with a Federal Law Enforcement Investigation/Retaliation

1. State Court Proceedings/Interferences/Retaliation

After July 10, 2024, having successfully knocked out Farrow Law and its computer network, the Threat Defendants noticed that Farrow began using an old computer with hard drives

[16] Ver. Comp., ¶454-458.
[17] *Id.* at ¶481-520.
[18] *Id.* at ¶337-363.
[19] *Id.* at ¶225-243.
[20] Ver. Comp., ¶745-756.
[21] *Id.*at ¶767-836; *see also* PNOF4, Ex. "C" - Aug. 22, 2024 Affidavit of Dr. Jane Doe.

to hand file documents and claims for cyber-stalking on behalf of his family and law firm and that proved too much of a risk that this family might get back on its feet and fight back. Thus, from mid-July 2024, through recent days, as alleged in painstaking detail in the Verified Complaint, the Threat Defendants embarked in a wildly brazen journey to use whatever means necessary to ensure their coverup of their coverup would not wind up in a court of law.

On July 15, 2024, Farrow hand-filed, on behalf of Plaintiffs, a Circuit Court Lawsuit in Miami Dade County, Florida, Case Number 2024-13000-CA-01[22] seeking a civil injunction pursuant to Florida's criminal stalking statute. Subsequently, the September 4, 2024 Amended Complaint and the September 30, 2024 Amended Injunction Motion were served upon Threat Defendants Heath Ritenour and John Ritenour on October 4, 2024. Upon the filing and service of these court documents, Plaintiffs were substantially retaliated against.[23]

On July 19 and August 6, 2024, Farrow filed a Domestic Circuit Court Petition and Supplemental Petition respectively against Defendant Steven Gunby requesting an injunction be entered to prevent further cyberstalking.[24] Orders for Threat Defendant Gunby to appear were entered, however, he did not appear at either the August 8, 2024 or the August 29, 2024 hearings. Surrounding each hearing, Farrow and Dr. Doe were the targets of retaliation.

From September 2024 through the day of the filing of this Motion, the Threat Defendants' Crisis Scams have gotten ever more desperate, dangerous and hazardous which have included: (1) hacking into Florida's eFiling Authority to deny Plaintiffs access to state courts[25]; (2) hacking into the Florida Bar Network[26]; (3) hacking into over a dozen computers, over a dozen cell phones, nearly twenty email accounts and approximately 40 different law firm networks[27]; and (4) interfering with Dr. Doe's internet access while she has been on call as the medical director of pediatric transplant at Jackson Memorial Hospital.[28]

---

[22] A copy of the July 15, 2024 Verified Original Complaint is incorporated herein and marked **Exhibit 3**.
[23] PNOF4, Ex "A" – October 22, 2024 Affidavit of Farrow and Corp. Rep. of Farrow Law.
[24] A copy of the July 19, 2019 Original Petition and August 6, 2024 Supplemental Petition are marked as Composite **Exhibit 4** to this Motion.
[25] Verified Comp., ¶841
[26] *Id.* at ¶837-840.
[27] *Id.*
[28] *See* Plaintiffs' Notice of Filing February 8, 2025 Affidavit of Dr. Jane Doe [D.E. 6] "PNOF6".

2. F.B.I. – Cooperation with Ongoing Federal Investigation

On September 3, 2024, Special Agents Morton and Schafer of the Federal Bureau of Investigation ("F.B.I.") Miami Field Office came to Farrow and Dr. Doe's home in response to their separate complaints. On September 4, 2024, Farrow met with the Special Agents at the Miami Field Office and provided them with some electronic devices and documents. On September 7, 10, 17, October 10, 17 and 25, 2024, November 8, 28 and December 12 and 18, 2024, Farrow has provided regular updates with respect to ongoing activities, supplemented with documentation and other evidence through subsequent F.B.I. portal links.[29] On November 2, 2024, Farrow met Special Agents Morton and Schafer at the F.B.I. Miami Field Office and reported some of his clients(s) were working with federal agencies in active domestic law enforcement field operations, and that one or more of these individual(s) electronic devices were compromised.[30]

3. Blocking Access to Courts/Interfering with Federal Law Enforcement

After Farrow's meeting with Special Agents Morton and Schafer at the FBI Miami Field Office in early November, the conduct escalated leading to the filing a November 11, 2024 Ex Parte Emergency Motion and the discovery that the Threat Actor Defendants had interfered with the Miami-Dade County, Florida CourtMap website to block and/or delay the delivery motions upload for court review on that system.[31]

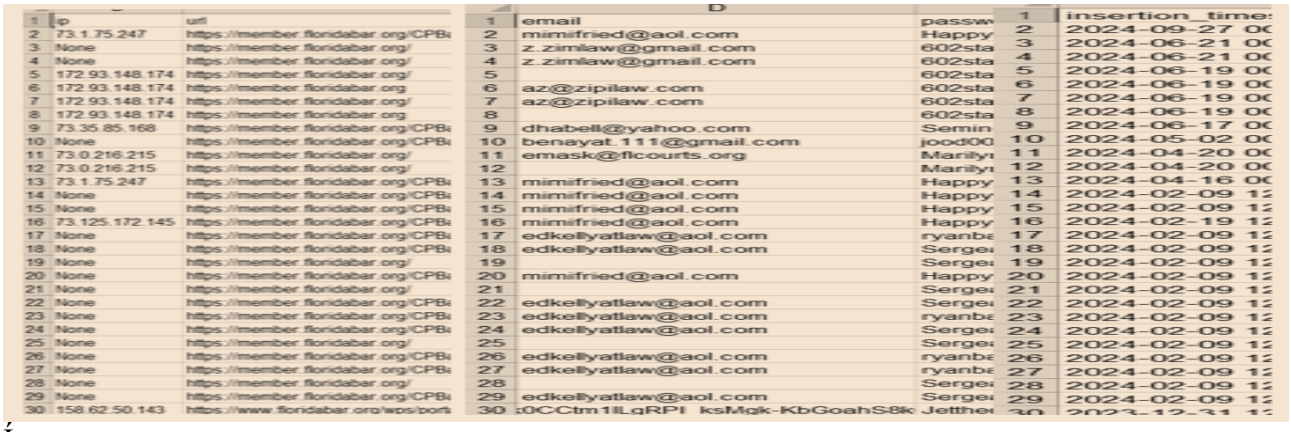
4. The Florida Bar and ePortal Authority's Network Breaches:

From August through December 2024, Plaintiffs encountered substantial issues logging into, filing and paying for state court filings.[32] Ultimately, the cause of these interferences were breaches into Florida's eFiling Authority's Network. On January 3, 2024, Farrow, Dr. Doe and Infant Doe hand-delivered evidence to the Florida Bar in Tallahassee contained within three spreadsheets showing the precise usernames, passwords, URLs and timestamps of unlawful infiltrations into its network and that of Florida's eFiling Authority.

---

[29] Certain Farrow's emails with Special Agents Morton and Schafer are Composite **Exhibit 5**.
[30] *See* PNOF4, Ex. "F."
[31] *See* PNOF4, Ex "F."
[32] *See* **Composite Exhibit 6** Florida's eFiling Authority's Computer Network compromises.

`



	ip	url
2	73.1.75.247	https://member.floridabar.org/CPB
3	None	https://member.floridabar.org/
4	None	https://member.floridabar.org/
5	172.93.148.174	https://member.floridabar.org/
6	172.93.148.174	https://member.floridabar.org
7	172.93.148.174	https://member.floridabar.org/
8	172.93.148.174	https://member.floridabar.org
9	73.35.85.168	https://member.floridabar.org/CPB
10	None	https://member.floridabar.org/CPB
11	73.0.216.215	https://member.floridabar.org/
12	73.0.216.215	https://member.floridabar.org/
13	73.1.75.247	https://member.floridabar.org/CPB
14	None	https://member.floridabar.org/CPB
15	None	https://member.floridabar.org/CPB
16	73.125.172.145	https://member.floridabar.org/CPB
17	None	https://member.floridabar.org/CPB
18	None	https://member.floridabar.org/CPB
19	None	https://member.floridabar.org/
20	None	https://member.floridabar.org/CPB
21	None	https://member.floridabar.org/
22	None	https://member.floridabar.org/CPB
23	None	https://member.floridabar.org/CPB
24	None	https://member.floridabar.org/CPB
25	None	https://member.floridabar.org/
26	None	https://member.floridabar.org/CPB
27	None	https://member.floridabar.org/CPB
28	None	https://member.floridabar.org/
29	None	https://member.floridabar.org/CPB
30	158.62.50.143	https://www.floridabar.org/wps/port

	email	passw
2	mimifried@aol.com	Happy
3	z.zimlaw@gmail.com	602sta
4	z.zimlaw@gmail.com	602sta
5		602sta
6	az@zipilaw.com	602sta
7	az@zipilaw.com	602sta
8		602sta
9	dhabell@yahoo.com	Semin
10	benayat.111@gmail.com	jood00
11	emask@flcourts.org	Marilyı
12		Marilyı
13	mimifried@aol.com	Happy
14	mimifried@aol.com	Happy
15	mimifried@aol.com	Happy
16	mimifried@aol.com	Happy
17	edkellyatlaw@aol.com	ryanbe
18	edkellyatlaw@aol.com	Sergei
19		Sergei
20	mimifried@aol.com	Happy
21		Sergei
22	edkellyatlaw@aol.com	Sergei
23	edkellyatlaw@aol.com	ryanbe
24	edkellyatlaw@aol.com	Sergei
25		Sergei
26	edkellyatlaw@aol.com	ryanbe
27	edkellyatlaw@aol.com	ryanbe
28		Sergei
29	edkellyatlaw@aol.com	Sergei
30	:0CCtm1lLgRPI_ksMgk-KbGoahS8k	Jetthe

	insertion_time
2	2024-09-27 0(
3	2024-06-21 0(
4	2024-06-21 0(
5	2024-06-19 0(
6	2024-06-19 0(
7	2024-06-19 0(
8	2024-06-19 0(
9	2024-06-17 0(
10	2024-05-02 0(
11	2024-04-20 0(
12	2024-04-20 0(
13	2024-04-16 0(
14	2024-02-09 1:
15	2024-02-09 1:
16	2024-02-19 1:
17	2024-02-09 1:
18	2024-02-09 1:
19	2024-02-09 1:
20	2024-02-09 1:
21	2024-02-09 1:
22	2024-02-09 1:
23	2024-02-09 1:
24	2024-02-09 1:
25	2024-02-09 1:
26	2024-02-09 1:
27	2024-02-09 1:
28	2024-02-09 1:
29	2024-02-09 1:

Í

https://tloxp.tlo.com/login.php	JMONROE@FLORIDABAR.ORG
https://clearwaterfl.mycusthelp.com/WEBAPP/_rs/(S(jxgqedtpbf5siyh3osj3	jmonroe@floridabar.org
https://mycusthelp.info/CLEARWATERFL/_rs/(S(tqubm3h0fs2pnk2ybouwvv	jmonroe@floridabar.org
https://pcso.govqa.us/WEBAPP/_rs/(S(ms3shltjz2rzjrxiuiwcg012))/Login.as	jmonroe@floridabar.org
https://pascocounty.mycusthelp.com/WEBAPP/_rs/(S(kpyyjn5mcafyq3kori:	Jmonroe@floridabar.org
https://colliercountyshofl.mycusthelp.com/WEBAPP/_rs/(S(oh4v2j1eigj2vp:	jmonroe@floridabar.org
https://ccso.mycusthelp.com/WEBAPP/_rs/(S(v3t015e5ofg41otq10z3uic2)	jmonroe@floridabar.org
https://colliercountyshofl.mycusthelp.com/WEBAPP/_rs/(S(oh4v2j1eigj2vp:	jmonroe@floridabar.org
https://azcourtdocs.gov/arizona/publicSignUp.admin	jmonroe@floridabar.org
https://ccso.mycusthelp.com/WEBAPP/_rs/(S(v3t015e5ofg41otq10z3uic2)	jmonroe@floridabar.org
https://pcso.govqa.us/WEBAPP/_rs/(S(ms3shltjz2rzjrxiuiwcg012))/Login.as	jmonroe@floridabar.org
https://stpetefl.mycusthelp.com/WEBAPP/_rs/(S(mqcsscnfgmnydhgvdxezri	jmonroe@floridabar.org
https://stpetefl.mycusthelp.com/WEBAPP/_rs/(S(mqcsscnfgmnydhgvdxezri	jmonroe@floridabar.org
https://hillsboroughsheriff.govqa.us/WEBAPP/_rs/(S(ku4srjpn4ax1eiml0c2t	jmonroe@floridabar.org
https://pascocounty.mycusthelp.com/WEBAPP/_rs/(S(kpyyjn5mcafyq3kori:	Jmonroe@floridabar.org
https://mycusthelp.info/CLEARWATERFL/_rs/(S(tqubm3h0fs2pnk2ybouwvv	jmonroe@floridabar.org
https://leecountysheriff.govqa.us/WEBAPP/_rs/(S(dztht24ymq1vebykx0dm	jmonroe@floridabar.org
https://azcourtdocs.gov/arizona/publicSignUp.admin	jmonroe@floridabar.org
https://securemail.csbflorida.com/s/e	jmonroe@floridabar.org
https://hillsboroughsheriff.govqa.us/WEBAPP/_rs/(S(ku4srjpn4ax1eiml0c2t	jmonroe@floridabar.org
https://login.microsoftonline.com/common/oauth2/authorize	jmonroe@floridabar.org
https://www.azcourtdocs.gov/arizona/publicLogin.admin	jmonroe@floridabar.org
https://tloxp.tlo.com/login.php	JMONROE@FLORIDABAR.ORG
https://login.microsoftonline.com/common/oauth2/authorize	jmonroe@floridabar.org
https://www.azcourtdocs.gov/arizona/publicLogin.admin	jmonroe@floridabar.org

5. Crisis Scam: From The Florida Bar to the Florida Supreme Court

The Threat Actors used both the breaches into the Florida Bar and Florida's eFiling Authority's Networks in a brazen scheme to jeopardize Farrow's License to Practice Law. In August 2024, both Farrow and Dr. Doe were contacted by a person claiming to be from FLA, except that they were, in fact, using an AI app to impersonate an FLA administrator whom Farrow had known for years.[33] Both Dr. Doe and Farrow's testimony in their Affidavits and Verified Statements from several court documents, unambiguously recount speaking with this 'FLA administrator' who specifically said that she had spoken with a lawyer working for the Florida Bar named "John Derek Womack."[34]

[33] *See. e.g.,* PNOF4, Ex. "C" Aug. 22, 2024 Aff. Dr. Doe; PNOF6, Feb. 8, 2025 Aff. Dr. Doe.
[34] In June 2024, Farrow Law was contacted via email by a potential client named "John Derek Womack" with an email address of jderek.com. At that time, Farrow had little, if any, direct contact with this person, they never became a client due to Farrow Law's effective closure on July 10, 2024 and Farrow only discovered an email from jderek.com in early February 2025.

Ultimately, Farrow contacted Mr. Womack who informed Farrow there were eleven Bar Complaints filed against him that required responses. On September 17 and 18, 2024, Farrow received the names of the alleged complainants from Mr. Womack and the alleged bar complaints from Ms. Mitchell. Immediately, Farrow noticed one or more names on the list where the individual or individual(s) that could not have logistically filed any bar complaint[35] – and upon further inquiry some of the purported 'bar complaints' were prepared by a user of the Florida Bar Network while they were signed into a Florida Bar user account.

On September 24, 2024, Farrow called Mr. Womack and indicated he was working on a court filing which would address the two central, if not exclusive issues, in all the alleged 'bar complaints' which were that communications and work stopped on files in or about June 2024. Mr. Womack agreed to accept the court filing as his initial 'official' response to the bar inquires after the upcoming October 9, 2024, injunction hearing against FTI's CEO and Threat Actor Defendant Steven Gunby. On October 14, 2024 Farrow served Mr. Womack and Ms. Mitchell as agreed, and on October 15, 2024, Ms. Mitchell send Farrow an email confirming receipt.[36]

On October 18, 2024, Farrow arrived at Farrow Law's Coral Gables Office to find a "3-Day Eviction Notice" posted on his door by Wiess Serota claiming to represent Farrow Law's landlord, Regus Management.[37] ***Just a few hours after receiving the "3-Day Notice" from Richard Wiess' law firm***, on **October 18, 2024**, Farrow received an email from Legal Assistant Mitchell entitled "**Files to Grievance Committee – Bar Counsel is Investigating Member-Notice of Assignment of Investigating Member**" addressed to "Chair [of Florida Bar Grievance Committee 17F] Richard Weiss, Weiss Serota at his Wiess Serota email address.[38]

Attached thereto was an October 15, 2024 letter from Mr. Womack to "Richard Jay Weiss, Chair" and the metadata on this letter indicates in was prepared on October 15, 2024, *after Legal Assistant Mitchell sent Farrow an acknowledged receipt of Farrow's October 14, 2024 Response*

[35] *See* PNOF4, Ex. "F".
[36] *See* Exhibit 7 Composite of Mitchell Emails.
[37] Wiess Serota is a Miami based law firm founded by Richard Wiess whose business address is 2525 Ponce De Leon Blvd. Coral Gables, Florida 33134 – which, as Farrow discovered in early December, is identical to Mr. Womack's business address.
[38] See **Exhibit 7** Composite.

the 'bar inquires".[39] On November 4, 2024, ***because this was an issue that could not be ignored and was an emergency with no responses or answers forthcoming from Womack***, Farrow drove from Miami to Tallahassee and hand-delivered updated responses to the alleged 'bar inquires', as well as, and all of his communications the F.B.I. so as to ensure that the Florida Bar received the same and such that there was no question he had 'responded to official bar inquires.

Notwithstanding, on November 12, 2024, Grievance Committee 17F Chaired by Mr. Wiess allegedly conducted a closed hearing regarding Farrow. On November 25, 2024, Mr. Womack a/k/the Threat Actors filed a Petition in the Florida Supreme Court stating falsely that Farrow failed to respond to office bar inquires and failed to provide any cause for his failure to do so styled: *The Florida Bar v. Jay Lewis Farrow, Florida Supreme Court*: Case Number: FSC: 2024-1681.

On December 17, 2024, Farrow timely responded to the Florida Supreme Court, Farrow received an email from the eFiling portal that his Response was 'rejected.' As such, on December 18, 2024, Farrow traveled in person to the Florida Supreme Court and hand-delivered and conventionally filed his Response ***as the consequences were far too serious to ignore***. On December 20, 2024, Farrow received an email which contained a link to an "Order" from the Florida Supreme Court indicating that Farrow's December 18, 2024 conventionally filed response was 'incomplete' and upon review of the online docket, Farrow's Response only had pages 1 through 21, with Page 21 having a number but no text and the remaining 13 pages, 22 – 24 were missing. Farrow refiled on December 22, 2024. On December 30, 2024, the Florida Bar filed an untimely Reply, but it was purported filed by a different attorney, Patrica Savitz, as "Staff Counsel." This Reply did not deny anything Farrow represented in his Response. On January 3, 2025, Farrow and Dr. Jane Doe were forced to end their first trip out of town short and drove to Tallahassee with Infant Doe where they hand-delivered all three spreadsheets of evidence and provided the Florida Bar with several means to contact them yet they have not heard back, and no calls or emails are returned since January 3, 2025.[40] Yet, on January 7, 2025, Farrow reached out to Ms. Savitz, with no response. On January 10, 2025, received a Notice of Substitution of Counsel which replaced Ms. Savitz with Randell Berman, however, he is also unresponsive. From mid-

[39] From October 18 through October 23, 2024, Ms. Mitchell sent numerous emails to Richard Wiess, yet she had been on vacation and out of the office for 'some time' but would be back on October 25, 2024 or the following Monday, October 28, 2024.

[40] Farrow is not accusing the Florida Bar of any wrongful conduct, quite the opposite, he has demonstrated that it is the victim of a cyber-attack. *See* PNOF4, Composite Ex., E(1) and E(2).

January through February 2025, Farrow focused on preparing the Verified Complaint, checking email and using his replacement phone sparingly to avoid Crisis Scams.

D. Affidavit Testimony Corroborating Facts, Events and Cyber-Interferences

1. Medical Director of Pediatric Transplant Dr. Doe Affidavits:

Dr. Jane Doe is the Medical Director of Pediatric Transplant, Adult Liver and Intestinal Transplant at Jackson Memorial Hospital and UM Heath's Miami Transplant Center. Dr. Jane Doe is also an Associate Professor of Pediatrics at the University of Miami Miller School of Medicine. On August 23, 2024 and February 8, 2025, Dr. Jane Doe executed Affidavits testifying as to her personal knowledge as to the cyber and non-digital attacks.[41] In her testimony, Dr. Doe details her evaluation of the facts, her experience of being the target, for example, of AI Voice Spoofing Calls which come through the same cell phone which is essentially the 911 number for organ transplant offers from around the country and a lifeline to physicians around the world treating pediatric patients experiencing organ failure.

2. Farrow and Farrow Law's Affidavit

On October 22, 2024, Farrow and Farrow Law executed an Affidavit filed in support of an Emergency Motion in the 2024 Family Circuit Court Case dated October 23, 2024.[42] While Farrow requested an emergency hearing 13 times from October 22, 2024 through November 10, 2024 by using what appeared to be the Miami-Dade County CourtMap portal.[43] However, the state court was unresponsive and seemingly never received, or never timely received, the requests for hearing as a function of the cyber-breaches directed to interfere with Plaintiffs' access to eFiling and uploading court documents to schedule hearings.

3. Farrow Law Clients' Affidavit Testimony Corroborate Identical Interferences with Devices and Emails

From August 30 through Present, the Three Clients who were able to reestablish contact with Farrow have submitted Affidavits herewith reporting that after contact was reestablished, they

[41] *See generally* PNOF6, Exhibit "C"; *See also* Feb. 8, 2025 Aff. of Dr. Doe.
[42] PNOF4, Ex "A."
[43] Exhibit 8 hereto.

experienced identical issues with the electronic communication devices and/or personal emails in addition to threats for physical altercations through email and/or text messages.[44]

E. Expert Report Summary Opinion and Source Documents

December 5, 2024 Expert Report Summary Opinion: The Expert Report Summary Opinion concludes: (1) Plaintiffs were the targets of an APT Cyber Attack commencing in 2000; (2) that there is a high probability that that FTI, in particular, orchestrated, planned, and executed the APT Cyber-Attack Against Plaintiffs; (3) the APT used specific types of TTPs; (4) the APT Cyber Attack utilized a 'lame' designation or Sitting Duck Cyber Attack to cause interferences with Farrow and Farrow Law's communications; (4) Official DNS Records cross referenced with open sources evidenced nearly 150 Web Domains and/or Hosting Server Domains reflect nefarious compromises as part of a pattern of using either domain hijacking, or IP spoofing; and (5) the subject domains purportedly were or are owned by **(a) thirty-four (34) law firms**, **(b) Florida's eFiling Authority**, **(c)the Florida Bar**[45], **(d) Florida's Lawyer's Assistant, Inc.**, (e) and networks associated with the **Jackson Memorial Hospital, Jackson Heath, and the UM Heath System** which were used for malicious purposes all in pursuit of their Ultimate Goals of causing Plaintiffs substantial damages as specifically defined herein.[46]

F. Verified Facts Related to Theft of Personal Confidential Information and Ongoing Threats to Farrow Law Clients

1. Florida Lawyers Assistance, Inc.

Farrow has been a proud member of FLA for nearly a decade. For years, Farrow had been asked to 'monitor' other lawyers going through their FLA programs. While sabotaging Farrow Law's Network in May, June and July 2024, the Threat Actor Defendants stole confidential information from the Farrow Law Network included information contained within the reoccurring calendar entries related to the Remote Video Conference Meetings of the Tuesday, 5:30 pm Fort Lauderdale Florida Lawyers Assistance Group which included the "RingCentral" link, and the

[44] Copies of the 'Client Affidavits' are attached hereto marked Composite **Exhibit 14**, however, the names of the Clients are being redacted as they have experienced retaliation.

[45] *See* **Composite Exhibit 9** representing redacted spreadsheets related to the compromise of the Florida Bar Computer network.

[46] *See* **Composite Exhibit 10** which are the individual Domain Name System reports for each respective domain suspected of being compromised by the Threat Defendants in furtherance of their Ultimate Goals. Plaintiffs' investigation is ongoing, as such, the included domains are non-exhaustive.

private emails of over forty (40) lawyers. Farrow's computer's hard drive evidenced at least three of them, such as one on Tuesday May 9, 2022.[47]

2. Ongoing Interferences with Farrow and Farrow Law's Clients

On February 5 and February 11, 2025, Farrow received purported filings from select cases which he was involved dating back to 2010, all of which contain pdfs which the Threat Defendants have used since at least December 2000 to upload malware payloads into Farrow and Farrow Law's protected computers. Since the Threat Defendants have manipulated Florida's eFiling Portal, Farrow and Farrow Law have no means to verify if former clients and current clients are impacted by these alleged filings.[48] On February 11, 2024, one of Farrow's clients received a threatening email which implied a possible physical altercation but specifically stated that 'all' of the clients emails and social media had been accessed and further threatened that if he shared the email, or attempted to resent passwords, there would be serious consequences.[49]

III. ARGUMENT AND MEMORANDUM OF LAW

On June 21, 2024, in the 2024 Federal Case, as he watched his law firm implode from massive cyber-attacks, undersigned filed the very first emergency motion after nearly twenty years of practicing before the Southern District of Florida. On November 2, 2024, undersigned was forced to call an emergency meeting at the F.B.I. Miami Field Office to report a proximity cyber-related breach which presented a clear and present danger to the safety of individual(s) working with federal law enforcement agencies in active domestic field operations which had never happened in nearly a decade of such service. Further, even though the Threat Defendants succeeded in a wild Crisis Scam to advance and file a November 25, 2024, Petition with the Florida Supreme Court seeking undersigned's immediate suspension, undersigned's first words to the Florida Supreme Court were owning his own failures to develop cyber-security habits leading to his family, his law firm's staff and his client's pain and suffering.

Additionally, in early January 2025, after undersigned and Dr. Doe came into information which came at extraordinary labor and expense that demonstrated how the Threat Defendants gained unauthorized access into the Florida Bar and the Florida's eFiling Authority's Networks, they provided it – in person - to the Clerk of the Florida Supreme Court and the Florida Bar before

[47] Exhibit 11.
[48] *See* Composite Exhibit "12" hereto which are printed emails regarding these case filings.
[49] Composite, Exhibit "13" hereto.

filing claims based, in part, on that evidence such as to allow those institutions to conduct their own investigations.[50] Pointedly, Plaintiffs Farrow and Dr. Doe have not gone around yelling fire and have done what first responders do if there is a fire – they assumed agency, worked solutions and showed up every day knowing that the work they had to do would ultimately benefit others, as well as, save their own lives or certainly the quality of them. However, while great strides have been made, their efforts are now akin to moving furniture on the Titanic given the relentless Crisis Scams and cyber-attacks by the Threat Defendants continue regardless of all their efforts to stop them.

In this Motion, Plaintiffs argue this Court has wide discretion to enter equitable orders directing a stopping or substantially curtailing the Threat Defendants lawless conduct. Regarding the wide latitude this Court has to fashion a remedy and reduce the same to a judicial order, Plaintiffs herein are not requesting for the entry of a common law injunction which would be premised on the longstanding traditional precedent under and Fed.R.Civ.P. 60(b). At the same time, Plaintiffs are not shying away from establishing: (1) a likelihood of success; (2) irreparable harm with (3) no adequate remedy at law; and (4) that the public interest is well-served.[51]

Point being, federal and state legislators have recognized that cyber-criminals have enjoyed the illusion that they are non-violent, and, at the same time, they use sophisticated defense evasion tactics operate in the shadows far removed from their victims and desensitized to how their ruthlessness causes substantial damages which are non-quantifiable in terms of money. To curtail their nefarious means and methods, the United States Congress and the Florida Legislature codified statutory equitable civil remedies within criminal laws such as the Computer Fraud and Abuse Act ("CFAA") 18 U.S.C. § 1030 *et. seq*. and Florida's Criminal RICO Act, Fla. Stat. § 895.01 *et. seq*. These statutory equitable remedies authorize this Court to venture from the rigid traditional common law injunction precedence, to effectuate the legislative intent to stop abusive cyber-crimes which, as here, substantially frustrate the prosecution of claims or otherwise are terrorizing and traumatizing victims such as Plaintiffs in this case.

---

[50] With respect to the interferences with the Florida Bar Network, the unlawful access to the Florida Bar's Network continues to cause irreparable harm in that Farrow has no means of contacting the Florida Bar securely.

[51] Plaintiffs contend that issue of any bond must be addressed, however, assert that under the circumstances of this case, that no bond be required, or that it be nominally set at $1.00.

It is undeniable, and perhaps understandable, that as a mother and father watching Infant Doe courageously fight through learning to pronounce words he was speaking back in May 2024, as they fight through their own struggles caused by inventorying the landscape of the damages caused by Defendants, they may be inclined to yearn for equitable relief beyond what is legally appropriate. However, there was a juncture where these parents accepted that, due to the level of sophistication of the cyber-hackers, the amount of money that has been spent and that continues to be by the Threat Defendants to intentionally cause pain while covering tracks, and the mere passage of time caused by relentless Crisis Scams, that it may very well be that the only relief they will ever get is neither equitable or judicial, *but in knowing their child saw them keep pursuing justice while holding true to their moral compass under the worse of circumstances*.

Thus, while Plaintiffs herein request this Court to exercise its discretion and employ serious and consequential equitable relief, they do so cognizant that ***courts of law are referees – not bodyguards*** - and that neither Congress nor the Florida Legislature intended the statutorily codified discretion to be a blank check. More likely, these provisions were a check to balance hundreds of years of tradition with the exponential evolution of criminal creativity using the information super-highway. As a 'check', Plaintiffs note that both statutory constructs emanate from criminally proscribed conduct which was determined to be so inherently destructive, dangerous and hazardous that is punishable as felonies with consequential prison terms. To that end, Plaintiffs requested relief respectfully asks for equitable relief which is both consequential *and* narrowly tailored to be the least restrictive means directed to enjoin the offensive conduct.

A. The Computer Fraud and Abuse Act

In the Verified Complaint, at Count III, Plaintiffs Farrow, Farrow Law and Dr. Jane Doe demand temporary and permanent injunctive relief, as well as, monetary damages pursuant to the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 *et seq*. Pursuant to 18 U.S.C. 1030(g), this Court has substantial discretion to fashion either traditional 'injunctive' or 'other equitable relief'. None of the Threat Defendants, or the Threat Actor Defendants for that matter, were or are past or current employees of Plaintiffs. As such, there are no factual issues related to the scope of authorization as none was ever provided by Plaintiffs to any Defendant. As such, in this case, there is zero doubt that Plaintiffs were the victims of: (1) the unauthorized accessing; (2) of protected computers belonging to Farrow, Farrow Law and Dr. Jane Doe; (3) with the intent (a) obtain information, (b) further a fraud, or (c) damage the computer or its data.

The only issue that is remotely at issue, is whether the Threat Defendants were and are the violators. Here, after reviewing Farrow and Farrow Law's actual computers, documentary evidence and official domain name system records, Plaintiffs' expert concluded there was a high probability that the Threat Defendants were and are behind the attack. Moreover, there is ample corroborating evidence, such using FTI's media outlets to attack Plaintiffs, the official DNS records of over 250 domains, and evidence connecting the sending of malware payloads through pdfs and links and modifications to Farrow Law's network which corroborate the Expert Report's findings.

Obtaining Information: Obtaining information through unauthorized access under the CFAA is broadly defined. Lawsuits concerning the theft or obtaining of confidential information, as here, meet the 'value' requirement. Factually, Plaintiffs' have a substantial likelihood of success on the merits that the Injunction Defendant stole the file related to the 2024 Federal Case, which contained information collected through costly investigations and professional hours spent preparing the evidence file related to the pending June 6, 2024 Injunction Motion.

Loss of Data or Damage to Computer: While Plaintiffs have alleged damages far in excess of $5,000 by calculating the damages caused, at the very least, by using authorized access to lock four computers belonging to Farrow Law, the costs paid by Dr. Doe and Farrow to replace computers, networks, software packages, and damages done to home computers and routers which respectively have caused more than $5,000 in damages to Farrow, Farrow Law and Dr. Doe. Damages also relate to medical treatment of Infant Doe.

Further a Fraud: Fraud under the CFAA is not like common law fraud. Essentially, the brightline test is simply whether 'unlawful', or unauthorized access, occurred. Here, unauthorized access was accomplished at the direction of the Threat Defendants, and Plaintiffs specifically alleged that the Threat Defendants knew or had constructive knowledge of the unauthorized access into Plaintiffs' protected computers.

Thus, Plaintiffs request that this Honorable Court find and determine that based upon Plaintiff's substantial likelihood of success on the merits, their suffering of irreparable harm for which there is no adequate remedy at law, to enjoin the Threat Defendants.

B. Florida's Criminal RICO Statute 'Civil Remedies' Provisions

In the Verified Complaint, Plaintiffs equitable relief in the form of a very limited restraining order under the Florida RICO Act § 895.05(6) entitled "Civil Remedies." Fla. Stat.

895.05(6) provides for injunctive relief for parties injured by violations of the Florida RICO Act and states in relevant part:

> Upon the execution of proper bond against damages for an injunction improvidently granted and a showing of immediate danger of significant loss or damage, a temporary restraining order and a preliminary injunction may be issued in any such action before a final determination on the merits. (emphasis added).

As recognized by Florida's Third District Court of Appeal: "Unlike its federal counterpart, the Florida RICO statute contains an express provision for private injunctive relief." *Banco Indus. de Venezuela, C.A. v. Mederos Suarez*, 541 So.2d 1324, 1326 (Fla. 3rd DCA 1989).[52]

In *Suarez*, plaintiff filed a four-count complaint against defendants, alleging common law fraud, conspiracy, debt, and Florida RICO violations. *Suarez,* 541 So.2d at 1325. Plaintiff alleged a complex scheme on the part of the defendants to take advantage of an import program which illegally leveraging the theft of $2.3 million. *Id*. Plaintiff filed a motion for a temporary injunction, enjoining the defendants from "disposing of 'any assets whatever their present form, representing, in whole or in part, funds derived from payments' from the racketeering scheme. *Id.* The trial court ruled that it could not issue the temporary injunction because "[Plaintiff] was unable, prior to discovery, to identify the stolen funds to assets held by the defendants." *Id*. at 1326.

The Third District Court of Appeal reversed, holding that plaintiff was entitled, as a matter of law, to a temporary injunction because it filed verified allegations which made a sufficient showing of immediate danger and significant loss, and posted an appropriate bond. *Id*. at 1327. Specifically, in a profound analysis of Section 895.05(6), the Third DCA held:

> As we read the plain language of the balance of section 895.05(6), the only requirements for a *preliminary* injunction under the Florida RICO Act, upon the filing of a verified complaint, are (1) posting a sufficient bond against damages, and (2) showing an "immediate danger of significant loss or damage." Where a plaintiff under the Florida RICO Act has filed a verified complaint, furnished a sufficient bond, and made the requisite showing, the statutory criteria for a preliminary injunction are satisfied.

[52]"The Florida RICO statute … specifically authorizes preliminary injunctions." *Bardfield v. Chisholm Properties Circuit Events, LLC*, 2009 WL 1659641, at *2 (N.D.Fla. June 12, 2009) (*citing* Fla. Stat. § 895.05(6)).

> Our construction is supported not only by the plain language of the statute, but also by the enabling clauses of the Act, which contain clear legislative findings that the national scope of organized crime is highly sophisticated and diverse and that the same patterns of unlawful conduct exist in Florida, making it "necessary to provide *new* criminal and civil remedies and procedures...." RICO Act, ch. 77–334, 1977 Fla. Laws 1399 (emphasis supplied).

Indeed, to use an analogy, Law Enforcement doesn't call ahead to alert RICO Defendants to see if it is a convenient time for them to "stop by." To be clear, based upon the filing of this verified motion, Plaintiffs need only: (1) show an immediate danger of significant loss or damage; and (2) post an appropriate bond. Here, Plaintiffs have demonstrated immediate danger of significant loss or damages, and that there is a high probability they have caused significant losses and damages. As reflected in the Threat Defendants' conduct and activities since September 2024 through present day, Plaintiffs have demonstrated imminent danger of significant loss or damages as Threat Defendants show no signs they are going to stop or are even deterred in the least by anything to this point. Plaintiff has also demonstrated, that based upon the conduct described, any bond should be nominal, and no more than $1.00.

WHEREFORE, in accordance with the above, Plaintiffs respectfully request this Court to enter an Order granting Plaintiff's Motion, and find that equitable relief is appropriate and necessary as argued herein above, first by prohibiting any Threat Defendant, or their agents, or contractors or affiliates, from attempting to or accessing computers owned by Plaintiffs, or hacking, accessing, and/or manipulating any cellphone, iPad, email account, social media account, or other electronic device directed to cause Plaintiffs significant harm and/or imminent harm or damages, and second, ordering the suspensions, conditional or otherwise, or restrictions upon the insurance licenses of Heath Ritenour, John Ritenour and Insurance Office of America, and conditional suspensions or restrictions to, IOA, Inc., IOA, LLC's and FTI's corporate charters and/or rights to conduct business in Florida. Finally, Plaintiffs request that any hearings related to this emergency motion be scheduled live as opposed to virtual, and that, each attorney that appears in this case provide at least one personal address for service of any and all court filnigs and discovery related matters. There be a nominal bond set, if any, of $1.00.

Respectfully submitted,

February 18, 2025

BY: **/s/Jay L. Farrow, Esq.,**
JAY L. FARROW, ESQ.
Florida Bar No. 625213
FARROW LAW FIRM
Attorneys for Plaintiffs
1 Alhambra Plaza, Penthouse
Coral Gables, Florida 33134
Telephone: (954) 805-1915
jaylewisfarrow@proton.me
eserviceflf@proton.me